

CLAIMS

What is claimed is:

5

1. A method for processing digital certificates within a data processing system, the method comprising:

determining a set of trust relations between a set of certificate authorities (CAs) in a trust web;

10

representing the set of trust relations in an adjacency matrix, wherein a cell in the adjacency matrix corresponds to a pair of certificate authorities;

15

performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities; and

20

performing an all-pairs-shortest-paths computation on the adjacency matrix to generate multiple sets of shortest trust paths between the certificate authorities.

2. The method of claim 1 further comprising:

initiating a secure communication with a requester;

receiving a digital certificate for the requester;

and

25

validating the digital certificate in accordance with an inter-CA trust path indicator and/or a shortest trust path.

3. The method of claim 2 wherein the digital

30

certificate is formatted according to X.509 standards.

4. An apparatus for processing digital certificates within a data processing system, the apparatus comprising:

means for determining a set of trust relations between a set of certificate authorities (CAs) in a trust web;

means for representing the set of trust relations in an adjacency matrix, wherein a cell in the adjacency matrix corresponds to a pair of certificate authorities;

means for performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities; and

means for performing an all-pairs-shortest-paths computation on the adjacency matrix to generate multiple sets of shortest trust paths between the certificate authorities.

5. The apparatus of claim 4 further comprising:

means for initiating a secure communication with a requester;

means for receiving a digital certificate for the requester; and

means for validating the digital certificate in accordance with an inter-CA trust path indicator and/or a shortest trust path.

6. The apparatus of claim 5 wherein the digital certificate is formatted according to X.509 standards.

7. A computer program product in a computer-readable medium for use in a data processing system for processing digital certificates, the computer program product comprising:

5 instructions for determining a set of trust relations between a set of certificate authorities (CAs) in a trust web;

instructions for representing the set of trust relations in an adjacency matrix, wherein a cell in the
10 adjacency matrix corresponds to a pair of certificate authorities;

instructions for performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a
15 trust path exists between a pair of certificate authorities; and

instructions for performing an all-pairs-shortest-paths computation on the adjacency matrix to generate multiple sets of shortest trust paths
20 between the certificate authorities.

8. The computer program product of claim 7 further comprising:

instructions for initiating a secure communication
25 with a requester;

instructions for receiving a digital certificate for the requester; and

instructions for validating the digital certificate in accordance with an inter-CA trust path indicator
30 and/or a shortest trust path.

9. The computer program product of claim 8 wherein the digital certificate is formatted according to X.509 standards.

2007-03-23 04:00

10. A method for operating certificate authorities within a data processing system, the method comprising:
establishing at a first certificate authority (CA) a trust relation with a second certificate authority; and
5 sending a trust relation update message to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web.

10 11. The method of claim 10 further comprising:
receiving at the first certificate authority from the central trust web agent a set of inter-CA trust path indicators that represent whether a trust path exists between the first certificate authority and other
15 certificate authorities in the trust web; and
receiving at the first certificate authority from the central trust web agent a set of shortest trust paths between the first certificate authority and other certificate authorities in the trust web.

20 12. The method of claim 11 further comprising:
initiating a secure communication with a requester;
receiving a digital certificate for the requester;
and
25 validating the digital certificate in accordance with an inter-CA trust path indicator and/or a shortest trust path.

30 13. The method of claim 12 wherein the digital certificate is formatted according to X.509 standards.

1004513.01000
20070925

14. An apparatus for processing information related to operations of certificate authorities within a data processing system, the apparatus comprising:

means for establishing at a first certificate authority (CA) a trust relation with a second certificate authority; and

means for sending a trust relation update message to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web.

15. The apparatus of claim 14 further comprising:

means for receiving at the first certificate authority from the central trust web agent a set of inter-CA trust path indicators that represent whether a trust path exists between the first certificate authority and other certificate authorities in the trust web; and

means for receiving at the first certificate authority from the central trust web agent a set of shortest trust paths between the first certificate authority and other certificate authorities in the trust web.

16. The apparatus of claim 14 further comprising:

means for initiating a secure communication with a requester;

means for receiving a digital certificate for the requester; and

means for validating the digital certificate in accordance with an inter-CA trust path indicator and/or a shortest trust path.

17. The apparatus of claim 16 wherein the digital certificate is formatted according to X.509 standards.

2004.12.04.1002

18. A computer program product in a computer-readable medium for use in a data processing system for processing information related to operations of certificate authorities within a data processing system, the computer
5 program product comprising:

instructions for establishing at a first certificate authority (CA) a trust relation with a second certificate authority; and

10 instructions for sending a trust relation update message to a central trust web agent, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web.

19. The computer program product of claim 18 further
15 comprising:

instructions for receiving at the first certificate authority from the central trust web agent a set of inter-CA trust path indicators that represent whether a trust path exists between the first certificate authority
20 and other certificate authorities in the trust web; and

instructions for receiving at the first certificate authority from the central trust web agent a set of shortest trust paths between the first certificate authority and other certificate authorities in the trust
25 web.

2007-01-01 10:00:00

20. The computer program product of claim 18 further comprising:

instructions for initiating a secure communication with a requester;

5 instructions for receiving a digital certificate for the requester; and

instructions for validating the digital certificate in accordance with an inter-CA trust path indicator and/or a shortest trust path.

10

21. The computer program product of claim 20 wherein the digital certificate is formatted according to X.509 standards.

2004.04.09 10:40:00

22. A method for operating certificate authorities within a data processing system, the method comprising:

receiving at a central trust web agent from a certificate authority (CA) a trust relation update message, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web, and wherein the trust relation update message indicates a change in a set of trust relations for the certificate authority; and

modifying a set of trust relations for the set of certificate authorities within the trust web based on an indicated request in the trust relation update message.

23. The method of claim 22 further comprising:

sending to the certificate authority from the central trust web agent a set of inter-CA trust path indicators that represent whether a trust path exists between the certificate authority and other certificate authorities in the trust web; and

sending to the certificate authority from the central trust web agent a set of shortest trust paths between the certificate authority and other certificate authorities in the trust web.

25. An apparatus for processing information related to operations of certificate authorities within a data processing system, the apparatus comprising:

means for receiving at a central trust web agent
5 from a certificate authority (CA) a trust relation update message, wherein the central trust web agent processes trust relation information for a set of certificate authorities within a trust web, and wherein the trust relation update message indicates a change in a set of
10 trust relations for the certificate authority; and

means for modifying a set of trust relations for the set of certificate authorities within the trust web based on an indicated request in the trust relation update message.

15 26. The apparatus of claim 25 further comprising:

means for sending to the certificate authority from the central trust web agent a set of inter-CA trust path indicators that represent whether a trust path exists
20 between the certificate authority and other certificate authorities in the trust web; and

means for sending to the certificate authority from the central trust web agent a set of shortest trust paths between the certificate authority and other certificate
25 authorities in the trust web.

20040401 10:04:00

28. A computer program product in a computer-readable medium for use in a data processing system for processing information related to operations of certificate authorities within a data processing system, the computer
5 program product comprising:

instructions for receiving at a central trust web agent from a certificate authority (CA) a trust relation update message, wherein the central trust web agent processes trust relation information for a set of
10 certificate authorities within a trust web, and wherein the trust relation update message indicates a change in a set of trust relations for the certificate authority; and

instructions for modifying a set of trust relations for the set of certificate authorities within the trust web based on an indicated request in the trust relation
15 update message.

29. The computer program product of claim 28 further comprising:

20 instructions for sending to the certificate authority from the central trust web agent a set of inter-CA trust path indicators that represent whether a trust path exists between the certificate authority and other certificate authorities in the trust web; and

25 instructions for sending to the certificate authority from the central trust web agent a set of shortest trust paths between the certificate authority and other certificate authorities in the trust web.

30. The computer program product of claim 28 further comprising:

instructions for representing the set of trust relations in an adjacency matrix, wherein a cell in the adjacency matrix corresponds to a pair of certificate authorities;

instructions for performing a transitive closure computation on the adjacency matrix to generate a set of inter-CA trust path indicators that represent whether a trust path exists between a pair of certificate authorities; and

instructions for performing an all-pairs-shortest-paths computation on the adjacency matrix to generate multiple sets of shortest trust paths between the certificate authorities.

20010943US1

31. A method for operating certificate authorities
within a data processing system, the method comprising:
generating trust paths at a central trust web agent
for certificate authorities in a trust web using a greed
5 algorithm; and

disseminating the generated trust paths by the
central trust web agent to the certificate authorities.

32. The method of claim 31 wherein the trust paths are
10 generated when a new certificate authority joins the
trust web or when a certificate authority changes a trust
relation with another certificate authority.

100451-011003

33. An apparatus for operating certificate authorities within a data processing system, the apparatus comprising:

means for generating trust paths at a central trust web agent for certificate authorities in a trust web using a greed algorithm; and

means for disseminating the generated trust paths by the central trust web agent to the certificate authorities.

34. The apparatus of claim 33 wherein the trust paths are generated when a new certificate authority joins the trust web or when a certificate authority changes a trust relation with another certificate authority.

2001-01-01 10:00:00

35. A computer program product in a computer-readable medium for use in a data processing system for processing information related to operations of certificate authorities within a data processing system, the computer
5 program product comprising:

instructions for generating trust paths at a central trust web agent for certificate authorities in a trust web using a greed algorithm; and

10 instructions for disseminating the generated trust paths by the central trust web agent to the certificate authorities.

36. The computer program product of claim 35 wherein the trust paths are generated when a new certificate
15 authority joins the trust web or when a certificate authority changes a trust relation with another certificate authority.

2004.01.01 10:00